㊦ (2)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-227152
(43)Date of publication of application : 03.09.1993

(51)Int.Cl. H04L 9/06
H04L 9/14
H04L 7/00
H04L 7/10

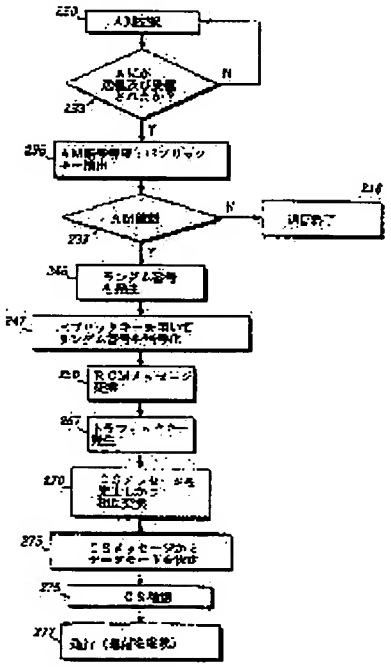
(21)Application number : 04-290804
(22)Date of filing : 05.10.1992

(71)Applicant : MOTOROLA INC
(72)Inventor : HARDY DOUGLAS A
LEWIS LESLIE K

(30)Priority
Priority number : 91 777870 Priority date : 16.10.1991 Priority country : US

(54) METHOD AND DEVICE FOR ESTABLISHING SECURITY COMMUNICATION LINK

(57)Abstract:
PURPOSE: To attain security communication among various tapes of user devices, using different encryption algorithm and encryption keys.
CONSTITUTION: This security communciation equipment includes a controller that uses any of common encryption algorithm sets for transmission and reception terminals to automatically select one of data encryption devices. A transmitter for encryption data and a receiver for encryption data are connected to a plurality of encryption devices. The controller automatically decides an encryption device to be adopted. The method to set up a security communication link includes a 1st message exchange stage deciding a common key production and the encryption method and a stage to confirm the validity of the communication terminal security through the comparison with other common message. Other message exchange stage for a traffic key, a state of inter-exchanging other message for synchronization confirmation and synchronization of security communciation between terminals and a state starting the security communciation are also used.



LEGAL STATUS

[Date of request for examination] 30.09.1999
[Date of sending the examiner's decision of rejection] 08.04.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平5－227152
(43)公開日　平成５年(1993)９月３日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
	7/00	Ａ	7928－5K		
	7/10		7928－5K		
			7117－5K	Ｈ０４Ｌ　9/ 02　Ｚ	

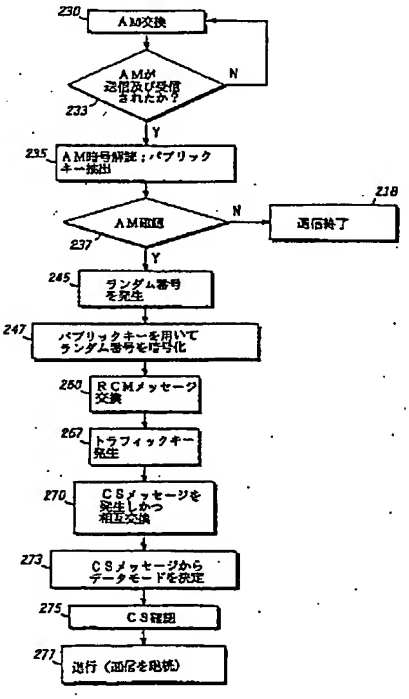
審査請求　未請求　請求項の数３(全 10 頁)

(21)出願番号　特願平4－290804
(22)出願日　平成４年(1992)10月５日
(31)優先権主張番号　７７７，８７０
(32)優先日　1991年10月16日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009597
モトローラ・インコーポレイテッド
MOTOROLA INCORPORATED
アメリカ合衆国イリノイ州シャンバーグ、イースト・アルゴンクイン・ロード1303
(72)発明者　ダグラス・エイ・ハーディ
アメリカ合衆国アリゾナ州85204、メサ、イースト・ゲイブル・アベニュー　2207
(72)発明者　レスリー・ケイ・ルイス
アメリカ合衆国アリゾナ州85260、スコッツデイル、イースト・ヴォルテア・アベニュー　8007
(74)代理人　弁理士　池内　義明

(54)【発明の名称】　機密通信リンクを確立する方法および装置

(57)【要約】
【目的】　異なる暗号アルゴリズム、暗号キーを用いる種々のタイプのユーザ機器間での機密通信を可能にする。
【構成】　機密通信用の装置は、送信および受信ターミナルに共通の暗号化アルゴリズムの１つを利用して、データ暗号化装置の１つを自動的に選択するコントローラを含む。暗号化データの送信機と、暗号化データの受信機が、複数の暗号化装置に結合される。コントローラは採用する暗号化装置を自動的に決定する。機密通信リンクを確立する方法は、共通のキー発生と暗号化方法を決定する第１メッセージ交換段階と、別の共有メッセージを比較して通信ターミナル機密の有効性を確認する段階とを含む。また、トラフィックキーのためのさらに別のメッセージの交換段階と、ターミナル間の機密通信の同期と同期確認用の別のメッセージを相互に交換する段階と、機密通信の開始段階とが用いられる。



【特許請求の範囲】

【請求項１】　第１（１０３，Ａ）および第２（１０９，Ｂ）ターミナル間に機密通信リンクを確立する方法であって、前記ターミナル（１０３，Ａ，１０９，Ｂ）が：両ターミナル（１０３，Ａ，１０９，Ｂ）内で使用可能な暗号化装置と通信モードとに関する情報を含む第１メッセージを交換する段階（２１１）；少なくとも１つのターミナル（１０３，Ａ，１０９またはＢ）において、共通のキー発生および暗号化の方法と、共通データ速度とを選択する段階（２１９，２２１，２２２）；ユーザの認証情報を含む第２メッセージを交換する段階（２３０）；トラフィック・キーを形成するためのデータを与える第３メッセージを交換する段階（２５０）；機密通信を同期させる第４メッセージを交換する段階（２７０）；および機密通信を開始する段階（２７７）；を含む手順に従うことを特徴とする機密通信リンクを確立する方法。

【請求項２】　ターミナル（１０３，Ａ，１０９，Ｂ）間に機密通信リンクを確立する方法であって、各ターミナル（１０３，Ａ，１０９，Ｂ）が：暗号化および解読機能を備えたアクセス・ドメインおよび機能メッセージを交換する段階（２１１）；認定されたユーザの認証データ、認定されたユーザのパブリック・キーを備えた認証メッセージを交換する段階（２３０）；第１乱数を含む第１乱数部メッセージを送り、第２乱数を含む第２乱数部メッセージを受け取り、トラフィック・キーを形成する段階（２５０）；暗号化同期メッセージを相互に交換する段階（２７０）；および機密情報相互交換を開始する段階（２７３，２７５，２７７）；を具備する手順に従うことを特徴とする機密通信リンクを確立する方法。

【請求項３】　いくつかの暗号化アルゴリズムのいずれかを用いて機密通信リンクを確立する装置（１００）であって：異なる暗号化アルゴリズムを利用する複数のデータ暗号化手段（ＫＧ１，．．．，ＫＧＮ）；暗号化されたデータを送る、前記複数の暗号化手段（ＫＧ１，．．．，ＫＧＮ）に結合された送信手段（１０３または１０９，ＡまたはＢ）；暗号化されたデータを受け取る、前記複数の暗号化手段（ＫＧ１，．．．，ＫＧＮ）に結合された受信手段（１０９または１０３，ＢまたはＡ）；およびある機密通信に関して、前記複数の暗号化手段（ＫＧ１，．．．，ＫＧＮ）のどれを採用するかを自動的に決定する制御手段（２１０）；を組み合わせて含むことを特徴とする機密通信リンクを確立する装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、保安または機密通信（secure communication）の改善された手段と方法とに関する。さらに詳しくは、異なった暗号アルゴリズムおよび／または暗号キーを採用している様々な種類のユーザ装置間の機密通信に関する。

【０００２】

【従来の技術】民間および軍事のユーザ間での機密通信に対する必要性が増大するのに合わせて、さまざまな暗号化技術とそれに対応する装置とが開発されてきた。無認可の(unauthorized)データ傍受が公益を害したり、個人の事業上の利益を害することがあるので、産業上，財政上，政府，警察，加入者媒体やその他の商業的活動および民間活動のための機密上の要件がより厳格になることにより、上記の必要性が強化されている。

【０００３】通常の暗号化されたデータには、コンピュータによる記録、電話での会話やその他の音声データ、遠隔測定データ、ファクシミリ送信、全地球測位システム（Global Positioning System）や加入者情報配布システムを含むさまざまな発信源からの地上と衛星との通信および衛星間の通信がある。データを暗号化する動機付けとしては、より均等なデータの混合（たとえば、「１」と「０」の不均衡な未暗号化列ではなく、「１」と「０」とが均等に混合された暗号データの通信）を促進することによる改善された信号対雑音比、加入者料金の強制、特権を与えられている会話のプライバシー、国家の機密事項およびコンピュータ犯罪を防ぎ同時に機密性を確保してユーザの認証を守るための商取引の完全性の維持などがある。

【０００４】情報監視や暗号解読法が発達したことにより、新しい暗号化アルゴリズムやそれに対応する装置の生産が誘導された。一例としてあげると、ただしこれに限らないが、現在広く用いられているいくつかのクラスの暗号化法には、いずれも米国商務省により発行された連邦情報処理規格（Federal Information ProcessingStandard Publications）ＦＩＰＳ４６－１に記述されるデータ暗号化規格（Data Encryption Standard　－ＤＥＳ）「データ暗号化規格」と、ＦＩＰＳ８１の「ＤＥＳ動作モード」があげられる。

【０００５】これらの多様な暗号化装置とアルゴリズムに共通の要素が、認可を受けた送信者および受信者が、暗号化を行いその後で意図されたメッセージを解読することができるある形態の暗号キー情報を共有するために必要とされる。

【０００６】電話などの機密通信のための従来の技術のパブリック・キー暗号化システムの欠点は、パブリック・キー・データ暗号化および解読が非常に速度の遅い処理であるということである。従って、パブリック・キー暗号化法は、より高速の暗号化技術のためのトラフィック・キーのような少量の情報の送信に用いられることが多く、無線チャンネルや電話回線などの公共の送信媒体において機密的な方法で用いられる。

【０００７】リアルタイムの双方向通信のための暗号化方法には、上記のＦＩＰＳ４６－１および８１に開示さ

れているさまざまな暗号化技術や、このような装置を供給する企業により開発されたその他の技術が含まれる。これらの方法により、双方がデータの暗号化のための適切なトラフィック・キーを有するかあるいはアクセスすることができれば、優れたデータの完全性を図ることができる。通常、この方法は、さまざまなデジタルまたはアナログ形式の入力データから形成されたデジタル・データのブロック上で動作する。

【０００８】

【発明が解決しようとする課題】ときには、複数の通信チャンネルを用いねばならないこともある。たとえば、逐次であろうと並列的であろうと２者以上の発信者と受信者とが関わる場合がそうである。すべてのユーザが同じ装置や、同じ暗号キーまたはアルゴリズムを持っていないことも多い。このような場合、暗号キーまたは暗号化アルゴリズムおよび装置が異なる余剰な装置が、各発信場所または受信場所で必要になることがある。このために通信装置や費用がよけいにかかる。さらに通信用装置の種類が可動式または携帯式であることが必要な場合は、複数の別個の機密通信用システムに合わせるために必要な電力要件，重量および大きな寸法を受け入れることはできない。

【０００９】１台の通信用ターミナルで複数の暗号化技術に対応しても、ユーザが他者の機能を知ることや、適切な機密通信装置を手動でユーザが選択することが必要になることもある。このため、採用される機密アルゴリズムやハードウェアの詳細に対するユーザの知識を増やし、認可されたユーザの情報をより多くの個人に広め、さらに機密通信を開始するために必要な詳細な構造に関知するユーザを増やすことになるので通信の機密性が損なわれることもある。このために機密通信リンクに影響を与えるエラーの危険性が増す。

【００１０】必要とされるのは、単独の装置内で複数の暗号化アルゴリズムおよび暗号キーに対応してリアルタイムの機密通信を迅速に行い、認可を受けた自己同期通信を多様な加入者間で確立および維持することができるようにする手段である。装置は小型軽量で、電力要件が低いことがさらに望ましい。

【００１１】

【課題を解決するための手段】本発明により、多様な暗号化システム間で暗号通信を実行するための新規の方法と装置とが開示される。

【００１２】機密通信用リンクを確立する方法は、両ターミナル内で使用することのできる暗号化装置と通信モードに関する情報を含む第１メッセージを交換する段階と、少なくとも１つのターミナル内で共通キーの発生および暗号化の方法と、共通データ速度とを選択する段階と、ユーザ認証情報を含む第２メッセージを交換する段階と、トラフィック・キーを形成するためのデータを提供する第３メッセージを交換する段階と、機密通信を同期させるための第４メッセージを交換する段階と、機密通信を開始する段階とを含む。

【００１３】機密通信のための装置には、異なる暗号化アルゴリズムを利用する複数のデータ暗号化手段と、暗号化されたデータを送信する、前記の複数の暗号化手段に結合された送信手段と、暗号化されたデータを受信する、前記の複数の暗号化手段に結合された受信手段と、前記の複数の暗号化手段のうちのどれを特定の機密通信のために採用するかを自動的に決定する制御手段とが含まれる。

【００１４】本発明の上記およびその他の特徴と利点とは、以下の詳細な説明と添付の図面とからさらによく理解されるであろう。

【００１５】

【実施例】ここで用いられる「暗号化」という言葉（encryption, enciphering, encoding ）は、生のテキストのメッセージを機密メッセージに変換することを意味し、「解読」（decryption, deciphering, decoding ）はその反対の処理を意味する。

【００１６】図１は、電話ネットワーク１２０、電話回線１０７、たとえば機密電話などの機密通信用ターミナル１０３，１０９を備えた機密通信システム１００を示す。動作においては、音声データが機密通信用ターミナル１０３，１０９のいずれかにおいてデジタル化される。ここでは「電話」または「通信用ターミナル」という言葉は、音声情報、ファクシミリ、映像、コンピュータ・データ、グラフィック・データおよびその組合せの情報を含み、ただしそれに限定されない情報を送信する任意の装置を含むものとし、「音声」、「データ」または「音声データ」という言葉はこれらとその他すべての種類の送信可能な情報を含むものとする。

【００１７】入力データは、ターミナル１０３または１０９で暗号化され、その後で、電話回線１０７および電話ネットワーク１２０を介して、順次、たとえばもう１つの機密通信用ターミナル１０９または１０３に送られる。ここで、暗号化とデジタル化の動作が逆に実行されて、元の入力データに相当する生のテキストのデータが作成される。無線リンク、パケット交換データ・ネットワーク、専用回線またはその他の通信用チャンネルなどの別の送信媒体を、電話回線１０７と電話ネットワーク１２０の代わりに用いても有用である。伝統的に、機密通信用ターミナル１０３，１０９に外付けあるいは内蔵することのできるモデムを用いて、電話回線またはその他の通信用リンク上でデジタル・データ・ストリームを通信する。

【００１８】本発明は、ターミナル１０３，１０９のいずれか一方あるいは両方の中に、両ターミナルが理解することのできるいくつかの可能なプロトコルの内の１つに従ってメッセージを暗号化および解読する手段と方法とを設けて、特性やプロトコルの異なるターミナル同士

が互いに通話を行うことができるようにすることにより従来の技術の問題を克服する。好適な実施例においては、プロトコルの選択は自動でありユーザにとって透過的（transparent)な形で実行される。好適な階層のプロトコルが含まれていることが望ましい。このように、本発明の多重プロトコル・ターミナルは、他の同じでないターミナルと通信することができる。

【００１９】図２は、機密通信用ターミナル１０３（および／または１０９）内のキー管理データ・ベース２１０の一例を概略図で示したもので、複数の暗号化キーと装置ＫＧ１ないしＫＧＮが配置されている。ＫＧ１ないしＫＧＮは、所定のＮ個のアルゴリズムのうちの１つに従い、選択された特定のアルゴリズムに適したキーを用いてメッセージの暗号化／解読を行う。制御手段２１５は、相互接続部２２０により複数の暗号化キーと装置ＫＧ１ないしＫＧＮに結合されており、特定の暗号化アルゴリズムを制御手段２１５により選択的に採用することができる。各機密通信ターミナル１０３，１０９には、１対のキー管理データ・ベース２１０が含まれ、一方は情報を暗号化して送信することを専門に行い、もう一方は、情報を受信して解読することを専門に行う。１つのキー管理データ・ベース２１０で両方の機能を行うこともでき、それが好ましい。２台（またはそれ以上）の通信用ターミナル１０３，１０９のうち１台だけが、複数の暗号化キーおよび装置ＫＧ１ないしＫＧＮを有する必要がある。もう１台のターミナルは、多重装置ターミナルにあるもののうち１つだけを持っていればよい。

【００２０】機密通信を開始することができるようにするには、ターミナル１０３，１０９を初期化しなければならない。本発明の好適な実施例により、初期化は、手動キー管理モードまたはパブリック・キー管理モードの２つのモードのいずれか一方により行う。パブリック・キー管理モードを用いると、その特定の通信用の独自の暗号キーの対を機密通信用ターミナルに物理的に運搬する（手で運ぶなど）不便さを避けることができる。

【００２１】図３は、ターミナルＡ，Ｂ（たとえばターミナル１０３，１０９）間の機密通信を、本発明によるパブリック・キー・モードで自動的に開始するためのメッセージ配列の一部を示す。図３に概略的に示されるように、パブリック・キー管理モードには、４つのメッセージの交換が含まれる。これらは（ｉ）アクセス・ドメインおよび機能（Access Domain and Capabilities: ＡＤ＆Ｃ）メッセージ２１１、（ｉｉ）認証メッセージ（Authentication Message: ＡＭ）２３０、（ｉｉｉ）乱数部メッセージ（Random Component Message: ＲＣＭ）２５０および（ｉｖ）暗号化同期（Cryptographic Synchronization:ＣＳ）メッセージ２７０である。これらのメッセージはそれぞれ、一連のバイトからなる所定の長さであることが望ましい。各バイトには、特定の種類（たとえば使用可能な暗号化装置，モデムの種類など）の情報が含まれていることが望ましく、たとえば、適切なバイト群を結びつけてメッセージを形成することなどにより、完全なメッセージが形成される。

【００２２】アクセス・ドメインおよび機能（ＡＤ＆Ｃ）メッセージ２１１は、この場合、以下のことを実行する。すなわち、キー管理モードの選択、選択されたキー発生器（ＫＧ）アルゴリズムの選択、ターミナルの認可の認定および他のターミナル機能（たとえばデータ速度）。図４は、図３のＡＤ＆Ｃメッセージ２１１を用いて本発明によりデータ速度と暗号アルゴリズムの適合を行う方法２００を示す流れ図である。

【００２３】図４に示されている方法２００は、ブロック２１１でアクセス・ドメインおよび機能（ＡＤ＆Ｃ）メッセージを交換する段階と、次のデータ速度をチェックする段階２１３、適切なデータ速度が識別されたか否かを判定する決定段階２１６およびすべてのデータ速度がチェックされたか否かを確認する段階２１７を含む反復ループ２１３，２１６，２１７と、決定段階２１６によりデータ速度の整合または適合が検出されたときにループ２１９，２２１，２２２に進む段階、または適合が発見できずにすべてのデータ速度がチェックされた場合に通信を終了させる段階２１８を備えて構成される。ループ２１９，２２１，２２２には、次の暗号化アルゴリズムをチェックする段階２１９と、適切な暗号化アルゴリズム（すなわち両ターミナルに共通のアルゴリズム）が識別されたか否かを判定する決定段階２２１と、すべての暗号化アルゴリズムがチェックされたことを確認する段階２２２とが含まれ、その後に、決定段階２２１が暗号化アルゴリズムの適合を検出した場合に動作を進める段階２２４と、適合を発見できずにすべての暗号化アルゴリズムをチェックし終った場合に通信を終了させる段階２１８とが続く。

【００２４】ＫＧ１およびＤＥＳと示されているキー発生器がただ２つだけあり、ＫＧ１およびＤＥＳが両方とも２つのターミナルに共通である場合には、ＤＥＳキーが好まれる状態が与えられている場合を一例として考える。ただしこれに限られるものではない。この状態では、方法２００は、４つの可能な結果のいずれかでＡＤ＆Ｃメッセージの交換を終了する。すなわち：（ｉ）２つのターミナル間で適合が発見できなかった場合に、呼は終了される；（ｉｉ）２つのターミナルにＫＧ１モードだけが共通の場合、ＫＧ１キー発生器が用いられる；（ｉｉｉ）２つのターミナルにＤＥＳキー発生器だけが共通の場合、ＤＥＳキー発生器が用いられる；（ｉｖ）ＤＥＳモードとＫＧ１モードの両方が両ターミナルに共通の場合、ＤＥＳキー発生器が用いられる。キー発生器機能のリストがもっと長い場合にも同様の結果が当てはまり、最も好適な共通の状況のキー発生器がその後の通信のために選択される。キー発生器の好適な順序は、ターミナルにあらかじめプログラミングされているか、あ

るいはＡＤ＆Ｃまたは他のメッセージの一部として送信される。

【００２５】ターミナルの機能は、メッセージ全体の中で、特定のバイトまたは（たとえば８個の）ビット群により示される。特定のバイトの特定のビット群を用いて、所定のプロトコルによりある機能を示す。たとえば、キー発生器機能バイトの先頭ビットは、占有の(proprietary) キー発生器のための機能を表わし、次のビットはＤＥＳタイプのキー発生器の機能を表わすように選択することができる。データ速度機能などに関しても、同様の用法を採用することができる。

【００２６】図５は、ターミナル認定の有効性を決定し、トラフィック・キーを設定し、暗号化／解読のプロセスを同期させる、図３の第２、第３および第４メッセージの交換を示す流れ図である。以下の段階が本発明により実行される。すなわち認証メッセージ（ＡＭ）の交換２３０、乱数部メッセージ（ＲＣＭ）の交換２５０および暗号化同期（ＣＳ）メッセージの交換２７０である。機密通信を行う（ブロック２７７）ための確認（ブロック２７５）があることも望ましい。

【００２７】図５は、認証メッセージ（ＡＭ）の交換の段階（ブロック２３０）、ＡＭ交換の確認の段階（ブロック２３３）、ＡＭ解読とパブリック・キー抽出の段階（ブロック２３５）およびＡＭ確認の段階（ブロック２３７）を含むループ２３０，２３３，２３５，２３７と、ＡＭ確認が失敗したときに通信を終了する段階２１８とを具備する。これらの段階の次に、乱数発生の段階（ブロック２４５）と、たとえばパブリック・キー暗号化を用いた乱数暗号化の段階（ブロック２４７）と、乱数部メッセージ交換の段階（ブロック２５０）と、トラフィック・キー発生の段階（ブロック２６７）と、暗号化同期メッセージの発生と送信の段階（ブロック２７０）と、データ・モード決定の段階（ブロック２７３）と、暗号化同期確認の段階（ブロック２７５）と、通信の継続の段階（２７７）とが続く。

【００２８】ＡＭ交換の段階（ブロック２３０）では、認定されたユーザ認証情報と、認定されたユーザ・パブリック・キーと、認定された情報の有効期限とを識別する情報が提供される。このメッセージは、パブリック・キー暗号法を用いて処理され、当技術では既知の手段によりメッセージの暗号化および解読を行う。

【００２９】各ターミナルでは乱数が発生され（ブロック２４５）、たとえばＡＭで受け取られたパブリック・キーを用いて暗号化された後で、他のターミナルに送られる。このため、交換（ブロック２５０で）される各乱数部メッセージ（ＲＣＭ）には、交換されたＲＣＭを発した通信用ターミナルにより発生された乱数が含まれる。この乱数は、機密通信用システムにおいて採用されるキー発生器のいずれかのためのトラフィック・キーを提供するのに充分な長さでなければならない。この第１乱数もまた、発信ターミナルに記憶され、他のターミナルから返された乱数部メッセージから解読された第２乱数と組み合わされる（ブロック２６７）。組み合わされた第１および第２乱数が、第３乱数を形成する。このとき、もう一方のターミナルでも同じことが起こっており、受け取られた（第１）乱数が内部で発生された（第２）乱数と組み合わされて、同じ第３乱数が形成される。第３乱数は、両ターミナルのために選択された（図４のブロック２２１）キー発生器のためのトラフィック・キーとして用いられ、最上位ビットからその中にロードされる。トラフィック・キー内の用いられなかったビットはすべて廃棄され、単一の装置が、変化するトラフィック・キー長を発生して、キー管理データ・ベース２１０（図２参照）内で複数のキー発生器の要件が異なる場合にも対応することができる。第１乱数は、たとえば、受け取られた認証メッセージ（ブロック２３０）に含まれる認定されたユーザ・パブリック・キーを用いて、ＲＣＭに組み込まれ交換される（ブロック２５０）前に暗号化される（ブロック２７０）。もう一方のターミナルから来た第２乱数にも、同じことが起こる。第１および第２乱数値を組み合わせる（ブロック２６７）方法として、当技術で既知のようにビット形式で乱数群を排他的ＯＲ処理することにより容易に実行することのできるモジュロ２の加算（modulo-two addition ）があげられる。しかし、当技術で既知の二進数を組み合わせる他の手段と方法とを用いることもできる。

【００３０】暗号化同期（ＣＳ）メッセージ２７０は、トラフィックの様式（音声、データなど）の情報と、必要に応じた暗号情報と、ＫＧ同期確認とを伝達する。線形帰還シフト・レジスタ（linear feedback shift register－－ＬＦＳＲ）を、暗号化装置の一部として用いることもできる。線形帰還シフト・レジスタは、開始値すなわちシードを必要とする。シードは、ＣＳメッセージ２７０の一部として必要になることがある暗号情報の一例である。ＬＦＳＲは、当技術では既知である。

【００３１】ＫＧ同期確認のための好適な方法は、既知のまたはチェック・データ・パターンの暗号化されたものであるデータを送信することである。これらのデータは、ＬＦＳＲにシードをロードして、送信側のＬＦＳＲとＫＧとを同期させ、その後で送信側のＬＦＳＲおよびＫＧを用いてシードおよびチェック・パターンを暗号化することにより発生される。これらの受信されたデータが、受信側の機密通信用ターミナルにより解読されると、受信されたシードは受信側のＬＦＳＲにロードされ、チェック・データ・パターンは、そこに記憶されているものと比較される。このパターン間の適合(match)が、機密通信用ターミナルの暗号化同期を示す。

【００３２】このようにこれらの段階により、複数の暗号化機能を有する機密通信用ターミナルが、自動的に（ｉ）所定の暗号化モードの階層から適切な暗号化モー

ドを選択して、（ｉｉ）共通のデータ速度を選択し、（ｉｉｉ）適切なターミナルの識別とユーザの認可とを実行し、（ｉｖ）パブリック・キーまたは他の方法を介してトラフィック・キーを交換し、（ｖ）暗号化通信の同期と確認とを実行することが可能になる。

【００３３】上記の段階は、大半がオペレータの目に見えない（transparent)方法で実行され、システムの機密性を増大させ、しかもオペレータは詳細な暗号化手順や方法に関する知識はより少なくて済む。

【００３４】手動キー管理モードにおいては、呼の設定手順は、図３および図４のアクセス・ドメインおよび機能（ＡＤ＆Ｃ）メッセージ２１１および図３および図５の暗号化同期（ＣＳ）メッセージ２７０の交換から構成される。

【００３５】図４のアクセス・ドメインおよび機能（ＡＤ＆Ｃ）メッセージ２１１は、どのキー管理モードを採用すべきか、どのＫＧアルゴリズムを選択すべきか、手動キー・データ・ベース内のどのトラフィック・キーを用いるべきか、またその他のターミナル機能を決定するための情報を提供する。

【００３６】暗号化同期メッセージ２７０の交換（図５）は、トラフィック・モード（音声、データなど）線形帰還シフト・レジスタのシード値および／またはＫＧ開始点を特定する情報を与えて、さらにＫＧ同期の確認を可能にする。

【００３７】＜具体化例＞以下に示すのは、本発明の手段と方法の一例である。図６は、ターミナル１０３（および／または１０９）に類似の機密通信用ターミナル６００を示し、モデム６１０が電話回線またはその他の通信用システム６０５と通信を行い、マイクロプロセッサ・コントローラ６２０に接続されている。マイクロプロセッサ・コントローラ６２０は、キー管理データ・ベース６３０に結合され、さらに６３３と識別されるキー発生器ＫＧ１と、６３７と識別されるＫＧ（たとえばＤＥＳ）と、スイッチ６４０と、音声またはデータ・リンク６４５とに結合されている。スイッチ６４０は、キー発生器６３３，６３７のどちらが音声またはデータ・リンク６４５をマイクロプロセッサ・コントローラ６２０、モデム６１０および通信用システム６０５に接続するために使用されるかを決定する。

【００３８】図７は、ＡＤ＆Ｃメッセージ２１１（図３および図４）のＫＧ機能バイト７１０およびモデム速度機能バイト７２０を示し、キー発生の様式と、データ速度と、与えらえた機密通信用ターミナル１０３，１０９（図１）により支援されるフォーマットとを示す。これらの例では、使用されないビットには“ＲＥＳ”と印が付けられ、使用されるビットと共に完全な機能バイト(Capabilities bytes)を形成する。優先順位が最も高いビットは、“ＲＥＳ”と記されていない最も左側のビットである。そのため、ＫＧ機能バイト７１０内では、優先順位が最も高いキー発生器はＤＥＳで、ＫＧ１は次に優先順位が高いキー発生器となる。同様に、データ速度の優先順位は、当技術では既知の標準のデータ速度により、９６Ｄ（最高）から４８Ｖ（最低）までの範囲となる。

【００３９】第１段階は、ＡＤ＆Ｃメッセージ２１１（図３および図４参照）の発生であり、これは図７の７１０，７２０のようにバイト群から構成され、ＡＤ＆Ｃメッセージ２１１を発信する装置の機能を記述する。次にＡＤ＆Ｃメッセージが交換され（図２のブロック２１１）、マイクロプロセッサ・コントローラ６２０に渡される。ここでメッセージは、段階２１３，２１６，２１７，２１９，２２１，２２２および２２４のように分解され、２つの機密通信用ターミナル間の対応する機能を決定する。対応関係の決定ができない場合は、通信は終了される（ブロック２１８）。適合すると、通信は進行する（ブロック２２４）。

【００４０】ＫＧ１およびＤＥＳと示されている２つの可能なキー発生器だけを考慮した場合は、ＤＥＳキー発生器に、両者が２つのターミナルに共通である（図７のバイト７１０のように）場合に、優先的な状況を与えると、ＡＤ＆Ｃメッセージの交換（ブロック２１１）は前述のように４つの可能な結果のいずれかで終了する。

【００４１】初期のモデム速度は、呼を起こした機密ターミナルにより設定される。このモデム速度は、両方の機密ターミナルに共通の別のモデム速度に変更することもできる。

【００４２】マイクロプロセッサ・コントローラ６２０（図６）は次に、モデム６１０を介して、第１認証メッセージ（ＡＭ）を送り、第２ＡＭを受け取る（図５のブロック２３０）。受け取られたＡＭは、処理され（ブロック２３５，２３７）、パブリック・キーを解読して、ＡＭを確認する(veryfy)。ＡＭが確認されない場合は、プロセッサは所定回数再試行を行うことができ、それでも確認できない場合は、図５のブロック２１８のように通信を終了する。

【００４３】次にマイクロプロセッサ・コントローラ６２０は、キー管理データ・ベース６３０（図２の２１０に類似のもの）から、キー発生器ＫＧ１ないしＫＧＮのうちの１つを採用して、乱数を発生し（図５のブロック２４５）、この乱数は受け取られたＡＭから解読された（ブロック２３５）パブリック・キーを用いて暗号化（ブロック２４７）される。暗号化された乱数とその他のデータが組み合わされて、乱数部メッセージ（random component message: ＲＣＭ）が形成され、このメッセージはＲＣＭのためのモデム６１０を介して遠隔地の（もう一方の）機密通信用ターミナルから交換される。受け取られたＲＣＭから得られた乱数は、その前に発生された乱数（ブロック２４５）と組み合わされて、ＡＤ＆Ｃメッセージから決定されたキー発生器のためのトラ

フィック・キーを形成する。乱数は、たとえば２個の二進数を排他的ＯＲ処理することにより実現される演算であるモジュロ２の演算を用いて加算することにより組み合わせることができる。

【００４４】その結果得られる（第３）の乱数を、ＡＤ＆Ｃメッセージの交換（ブロック２１１）により選択されたＫＧ内に、最上位ビットからロードする。

【００４５】マイクロプロセッサ・コントローラ６２０は、送信側の線形帰還シフト・レジスタのためのシードとして用いられる別の乱数を発生する。チェック・パターンが暗号化されて、ＣＳメッセージの一部として送信される（ブロック２７０）が、これには遠隔地の（もう一方の）ターミナルの受信側ＬＦＳＲおよび／またはＫＧのためのシード（複数）も含まれている。遠隔のターミナルから受け取られたＣＳメッセージ（ブロック２７０）には、第１（発信側の）機密通信用ターミナルの受信側ＬＦＳＲおよび／またはＫＧにより用いられるシードが含まれる。これは受信されたＣＳメッセージから解読され、受信されたチェック・パターンを解読するために用いられる。遠隔のターミナルにおいても同様の動作が実行される。チェック・パターンが適切に解読され（ブロック２７５）、記憶されたデータ・チェック・パターンに照合されると、望ましいメッセージの機密通信が進行される（ブロック２７７）。チェック・パターンの解読がうまく行かない場合、キー発生器に再度乱数がロードされ、ＣＳメッセージの交換（ブロック２７０）が再試行される。

【００４６】本発明の好適な実施例においては、マイクロプロセッサ・コントローラ６２０は、モトローラ社（アリゾナ州、フェニックス）製の２個のタイプ６３０３マイクロコントローラ・チップと、タイプＤＳＰ５６００１高速デジタル信号処理チップとから構成される。第１のタイプ６３０３のマイクロコントローラは、すべての信号流れタスクを行い、図４および図５の各々の段階をいつ行うかを決定し、第２のタイプ６３０３のマイクロプロセッサ・チップは、各メッセージ２１１，２３０，２５０，２７０の内容を判定し、タイプＤＳＰ５６００１のチップは、たとえばパブリック・キーに暗号化されたデータの暗号化と解読に関わる数値集約的な計算と、その他の同様の演算上の作業とを行う。モデム機能の好適な実施例はタイプＶ．２６、あるいはタイプＶ．３２である。これらのタイプのモデムは、モトローラ社の子会社であるUniversal Data Systems（アリゾナ州、Huntzville）により販売されている。しかし、その他のモデムや通信方法も用いることができる。

【００４７】

【発明の効果】上記の説明に基づき、本発明が前述された問題を解決し、目的を達成して、しかも、とりわけここに示した実質的な利点を有することが当業者には明白であろう。その利点とは次のものである：（１）異なる暗号化アルゴリズム、キー変数およびキー変数長を採用する異なる種類の機密データ通信用システム間で、複数の暗号化機関を含む単一の装置により、機密通信を行うことができる、（２）所定の階層のアルゴリズム、キー、通信モードなどを与えて、機密性を増大する、（３）ユーザの目に見えないようにすることができる。これらの機能を１台の装置に備えることにより、本発明は装置の電源要件と費用とを最小限に抑えて、小型の装置を提供する。

【００４８】本発明のもう１つの利点は、機密情報プロトコルとキー変数交換を自動化することにより、システムの操作に関するユーザの詳細な知識に対する必要性を最小限に抑えていることである。このために、機密通信用ターミナルの操作が簡単になる。さらに、システムの動作を記述する情報の配布に対する必要性が小さくなり、そのために詳細なシステムの知識の露出を最小限に抑えてさらに機密性が増す。

【００４９】本発明は特定の要素、構造および段階に関して説明されたが、これらの選択は説明の便宜を図るためのもので、制限するためものではない。また、以上の説明に基づき、本発明は他の要素、装置および処理段階を選択した場合にも適用されることが当業者には理解いただけよう。また、本開示に基づき当業者が考えられるであろう、本発明の範囲と精神とに入る上記その他の変形も、添付の請求項に含まれるものとする。

【図面の簡単な説明】

【図１】本発明による公共電話システムを用いた機密通信システムの概略図である。

【図２】本発明によるキー管理データ・ベースの概略図である。

【図３】本発明により機密通信を開始するためのメッセージ配列の一部の説明図である。

【図４】本発明の好適な実施例によるデータ速度と暗号化アルゴリズムの適合動作を示す流れ図である。

【図５】本発明の好適な実施例により機密通信を確立するための図３のメッセージ交換の一部をさらに詳細に示した流れ図である。

【図６】本発明の好適な実施例による機密通信用ターミナルの一例の概略図である。

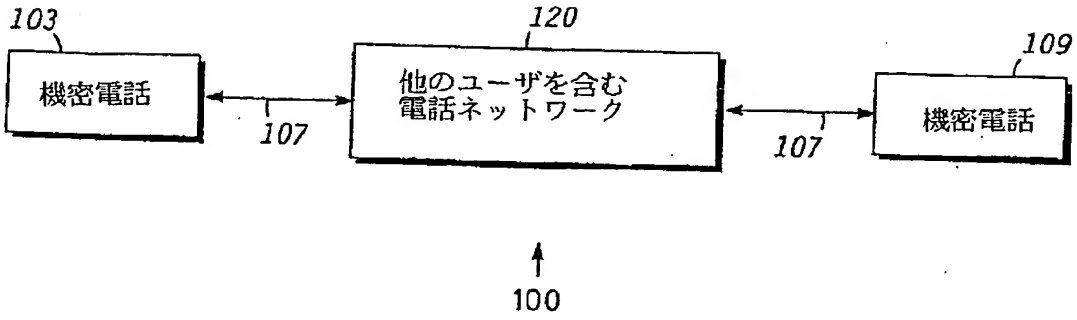
【図７】本発明の好適な実施例による、送信および受信ターミナル間で交換されるメッセージにおいてキー発生機能を表わすビットの割当てを示す説明図である。

【符号の説明】

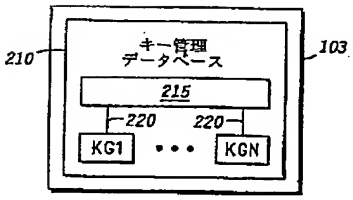
１００　機密通信システム
１０３，１０９　機密通信ターミナル
１０７　電話回線
１２０　電話ネットワーク
２１０　キー管理データベース
２１５　制御手段
２２０　相互接続部

２１１　アクセス・ドメインおよび機能メッセージ　　２５０　乱数部メッセージ
２３０　認証メッセージ　　２７０　暗号化同期メッセージ

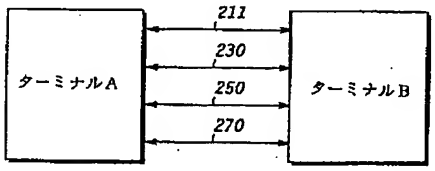
【図１】



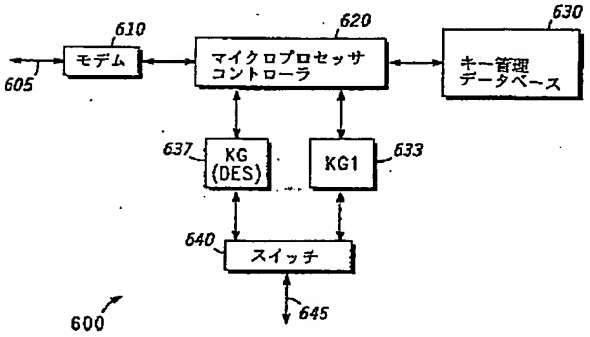
【図２】



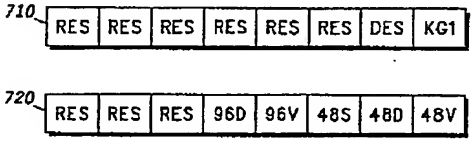
【図３】



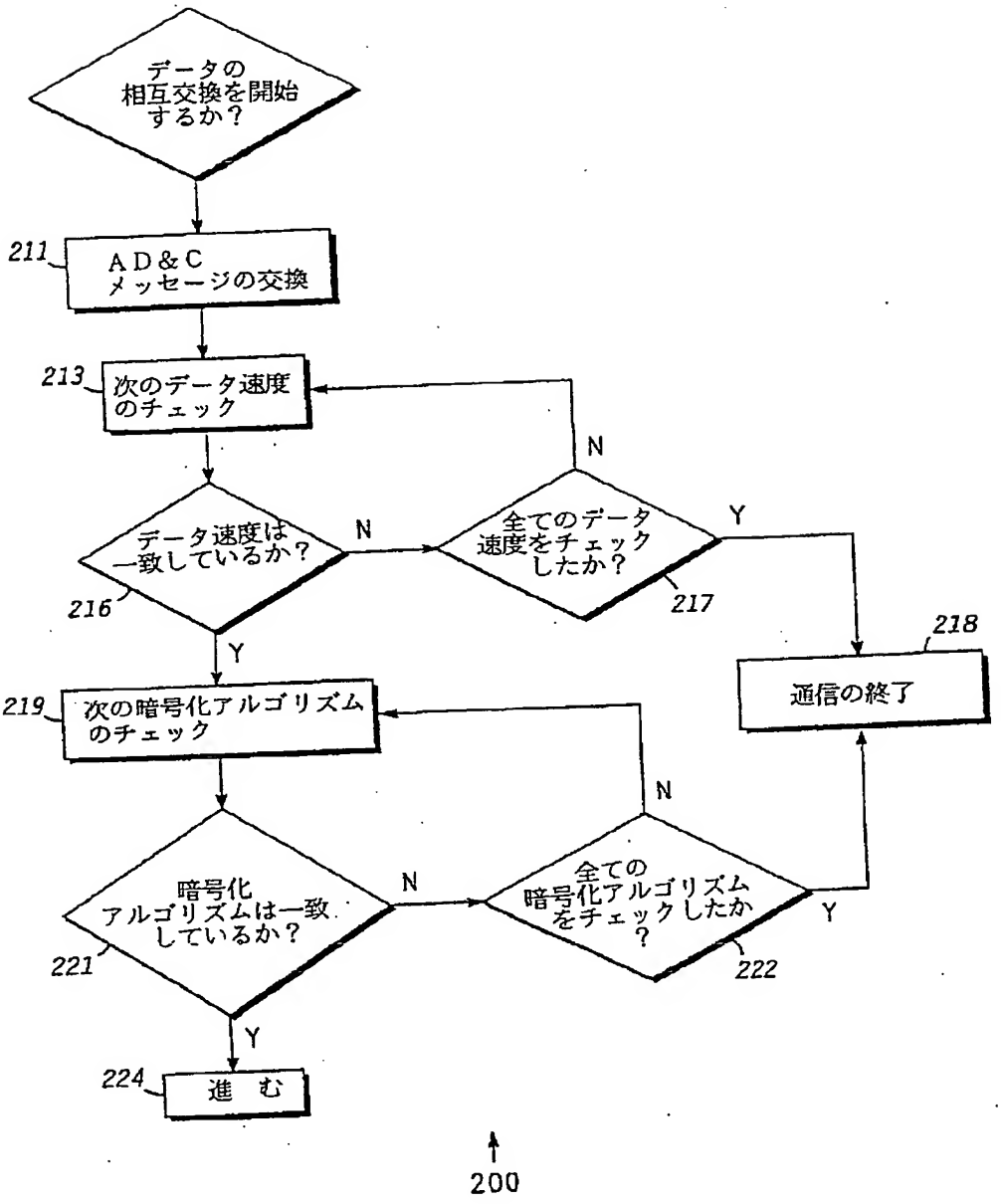
【図６】



【図７】



【図4】



【図５】